

**IN THE SPECIFICATION**

Please amend the paragraph that begins at page 6, line 1 as follows:

5       The practical benefit of the inventive idea results from an assumption that  
typically, the operational subCAs will not get compromised. Assuming this, a [a]  
batch of revocation lists manifesting no revocations can be generated and  
signed. These pregenerated CRLs (root CRSs) can then be stored outside the  
high-security vault and, in case of no subCA compromises, published periodically  
10       one at a time to the directory system where the PKI clients can automatically  
fetch them.

Please add the following new paragraphs beginning at page 7, line 27 just before the  
heading DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS:

15       Figure 2 is a flowchart of an embodiment of the invention.

Figure 3 is a flowchart of another embodiment of the invention.

Figure 4 is a diagram of the hardware and software architecture of an  
embodiment of the invention.